



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Am

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/724,972	11/28/2000	Stephen M. Trimberger	X-805-9 US	7821

24309 7590 05/13/2005

XILINX, INC
ATTN: LEGAL DEPARTMENT
2100 LOGIC DR
SAN JOSE, CA 95124

EXAMINER

NGUYEN, MINH DIEU T

ART UNIT PAPER NUMBER

2137

DATE MAILED: 05/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/724,972

Applicant(s)

TRIMBERGER ET AL.

Examiner

Minh Dieu Nguyen

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 20 September 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-28 is/are pending in the application.
- 4a) Of the above claim(s) 7 is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-4, 8-13, 16-23, 26-28 is/are rejected.
- 7) ☒ Claim(s) 5, 6, 14, 15, 24 and 25 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- ☐ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 9/20/04, 2/3/05.
- ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- ☐ Notice of Informal Patent Application (PTO-152)
- ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the communication dated September 20, 2004 with the cancellation of claim 7 and the addition of claims 11-28.

Claims 1-28 are pending.

Response to Arguments

2. Applicant's arguments, filed September 20, 2004, with respect to the rejection(s) of claim(s) 1-10 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Kean and the admitted prior art.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1-4, 8-13, 16-23 and 26-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kean, US 2001/0015919 in view of admitted prior art.

a) As to claim 1, Kean discloses a method to prevent monitoring of the configuration data for the field programmable gate array comprising a decryptor (Figure 5, element 64) for decrypting an encrypted bitstream (page 1, paragraph 0009); and a decryption algorithm implemented by the decryptor (page 8, paragraphs 0104-0107). Kean discloses the decryption algorithm uses unique key in the ID register (Figure 5, element 62) for decrypting the encrypted bitstream. Kean also discloses the security circuit (Fig. 5, element 64) may encrypts/decrypts the configuration data using the triple data encryption standard algorithm in a cipher block chaining (CBC) mode algorithm (page 2, paragraphs [0015] and [0023]). Kean further discloses cipher block chaining mode with the required initial value saved as part of the header before the configuration information (page 8, paragraphs [0107-0112] and in CBC decryption, the initial value is used for starting the chaining.

Kean does not disclose an address indicator for indicating an address into which configuration data will be loaded.

The admitted prior art discloses an address indicator for indicating an address into which configuration data will be loaded (Fig. 2d, element 0001).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of address data into which configuration data will be loaded from the address indicator, as admitted prior art teaches, in the system of Kean so as to indicate the types of control information that can be loaded into the registers.

b) As to claims 2, 12 and 22, Kean discloses the address in the configuration bitstream indicates an initial address in configuration memory at which configuration data is to be stored (page 7, paragraph [0098]).

c) As to claims 3, the admitted prior art discloses the initial address indicator is a frame address for indicating a starting frame of the PLD into which configuration data will be loaded (Fig. 2d, element 0001).

d) As to claims 4, 13 and 23, Kean discloses the PLD wherein the decryption algorithm comprises the DES algorithm (page 2, paragraph 0020).

e) As to claims 8-10, Kean discloses a value in the bitstream is loaded in the address indicator (i.e. initial value, page 8, paragraph [0112]), wherein the value is encrypted (claim 9) or unencrypted (claim 10).

f) As to claims 9-10, 16-17 and 26-27, the examiner takes official notice that normally data is sent in the plain text, when there is a need to securely protect data, the use of encryption is quite well known in the data encryption art.

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of encryption to encrypt certain data in the system of Kean and admitted prior art so as to securely protect data.

g) As to claims 11 and 20, Kean discloses a method and apparatus for secure configuration of a field programmable gate array (FPGA) comprising storing a plurality of decryption keys in storage elements of the PLD (i.e. multiple keys in triple DES where they are stored in ID register, in nonvolatile memory, page 2, paragraphs [0012], [0015], [0019-0021]); receiving a configuration bitstream at the PLD, wherein the

Art Unit: 2137

configuration bitstream includes control data (Fig. 6, elements 80-84) and configuration data (Fig. 6, element 86) and at least the configuration data is encrypted (page 2, paragraph [0011]); decrypting the configuration bitstream in the PLD using the address from the configuration bitstream and the plurality of decryption keys whereby a decrypted configuration bitstream is generated (Fig. 5, element 64; page 1, paragraph [0009]; page 8, paragraphs 0104-0107). Kean discloses the security circuit (Fig. 5, element 64) may encrypts/decrypts the configuration data using the triple data encryption standard algorithm (i.e. plurality of decryption keys) in a cipher block chaining (CBC) mode algorithm (page 2, paragraphs [0015] and [0023]). Kean further discloses cipher block chaining mode with the required initial value saved as part of the header before the configuration information (page 8, paragraphs [0107-0112] and in CBC decryption, the initial value is used for starting the chaining; and storing configuration data from the decrypted configuration bitstream in configuration memory of the PLD page 7, paragraph [0095]).

Kean does not disclose control data includes an address that references configuration memory of the PLD.

The admitted prior art discloses control data includes an address that references configuration memory of the PLD. (Fig. 2d).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of control data including an address in referencing configuration memory of the PLD, as admitted prior art teaches, in the system of Kean so as to indicate the types of control information that can be loaded into the registers.

h) As to claim 18, Kean does not disclose disabling readback of configuration data from the PLD after storing the configuration data in configuration memory.

However, Kean discloses reading back of configuration data with an encryption key to form a secure bitstream (page 6, paragraph [0072]). This concept of securely protect configuration data would be implemented as to disable readback of configuration data after storing the configuration data in configuration memory.

i) As to claim 19, Kean does not explicitly disclose disabling partial configuration of the PLD in response to decryption of the configuration bitstream. However, Kean discloses a field programmable gate array which supports partial reconfiguration may be programmed by a sequence of bitstream fragments, each bitstream fragments can be loaded and verified independently and would have its own crypto checksum (page 10, paragraph [0135]). Kean also discloses each encrypted bitstream will have a different initial value applied so this does not compromise security (page 10, paragraph [0136]). This concept of preventing attack would be implemented to disallow partial reconfiguration once configuration with decryption is started.

j) As to claim 21, Kean discloses a programmable logic device comprising a configuration memory (Fig. 5, element 14); a key management circuit adapted for storage of a plurality of keys (i.e. multiple keys in triple DES where they are stored in ID register, in nonvolatile memory, page 2, paragraphs [0012], [0015], [0019-0021]); a configuration circuit (Fig. 5, element 12) coupled to the configuration memory and to the plurality of storage elements (Fig. 5, element 62), the configuration circuit adapted to configure the configuration memory with an input configuration bitstream (Fig. 5,

Art Unit: 2137

elements 20, 64), wherein the configuration bitstream includes control data (Fig. 6, elements 80-84) and configuration data (Fig. 6, element 86) and at least the configuration data is encrypted (page 2, paragraph [0011]); and a decryptor (Fig. 5, element 64) coupled to the configuration circuit (Fig. 5, element 12) and to the plurality of storage elements (Fig. 5, element 62), the decryptor configured to decrypt, responsive to the configuration circuit, an input configuration bitstream using the address from the configuration bitstream and a plurality of decryption keys stored in the plurality of storage elements (Fig. 5, element 64; page 1, paragraph [0009]; page 8, paragraphs 0104-0107). Kean discloses the security circuit (Fig. 5, element 64) may encrypts/decrypts the configuration data using the triple data encryption standard algorithm (i.e. plurality of decryption keys) in a cipher block chaining (CBC) mode algorithm (page 2, paragraphs [0015] and [0023]). Kean further discloses cipher block chaining mode with the required initial value saved as part of the header before the configuration information (page 8, paragraphs [0107-0112] and in CBC decryption, the initial value is used for starting the chaining; and storing configuration data from the decrypted configuration bitstream in configuration memory of the PLD page 7, paragraph [0095]).

Kean does not disclose programmable logic circuitry coupled to the configuration memory.

The admitted prior art discloses programmable logic circuitry coupled to the configuration memory (Fig. 1, element 11).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of programmable logic circuitry coupled to the configuration memory as the admitted prior art discloses in the system of Kean so as to provide programmable logic for PLD to perform desired functions.

- k) As to claim 28, please see above addressed claims 18 and 19.

Allowable Subject Matter

5. Claims 5-6, 14-15 and 24-25 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873. The examiner can normally be reached on M-F 6:00-2:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on 571-272-3868. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

Application/Control Number: 09/724,972
Art Unit: 2137

Page 9

Minh Dieu Nguyen
Examiner
Art Unit 2137

mdn
5/5/05

A handwritten signature in black ink, appearing to read "Andrew Caldwell". The signature is fluid and cursive, with a large initial "A" and a stylized "C" at the end.

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER